

## RESPONSE

### Claims Status

Claims 1 – 21 were originally filed in this application. A restriction requirement was issued on February 7, 2005, and in a response thereto, Applicant elected to pursue claims 1 – 18 in this application. An office action was issued on September 19, 2005, rejecting claims 1 – 18, and Applicant filed a response thereto on December 7, 2005, in which claims 1 – 4, 9, 11, 16 and 18 were amended. A final office action was issued on January 27, 2006, maintaining the objections of the previous action. In this response, Applicant has amended independent claims 1 – 4, 11 and 18. Support for the amendments can be found throughout the originally filed specification and claims, and, for example, at paragraph [0014]. No new matter has been added.

### Claim Rejections

In the current Action, claims 1 – 18 were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent Serial No. 6,233,577 to Ramasubramani et al. (“Ramasubramani”).

Applicants respectfully submit that the claims as amended are patentable over the cited reference.

### Ramasubramani

Ramasubramani is directed generally to a centralized certificate management proxy server useful for mobile devices. The proxy server facilitates “obtaining certificates asynchronously, apart from the tradition of obtaining certificates in local devices that normally have sufficient computing power.” Col. 7, line 63 – 66. The Ramasubramani proxy server stores certificates in a table so that a mobile device can make use of the certificates even if it lacks sufficient processing power to do so.

Each Ramasubramani mobile device “has its own unique device ID that corresponds to a subscriber ID.” Col. 7 lines 1-5. The user’s account on the proxy server is “indexed by the device ID or the subscriber ID and identified by an address identifier such as a URL” and “compris[es] user info, a certificate list, and a private key list.” Col. 7 lines 10-14.

A user can use a PC (not the mobile device) to access the user's account on the proxy server: "the user may use the PC which has preferably a sufficient computing power and equipped with a more familiar HTML browser to establish a communication session using HTTP and the URL to the account." Col. 8 lines 54-57. When accessing his account from a PC, the user employs a username and password: "If the entered username and password are matched, the authorization is granted so that the user or (sic) the PC is permitted to access the account. Col. 8 lines 63-65.

### Claims 1 – 3

Independent claims 1, 2 and 3 each recite, in part, setting access privileges to the resource for a cluster of users . . . wherein the cluster is indicative of the user's role in an organization and the access privileges represent data access rights of members of the cluster to the resource, and locating the access privileges in response to the received request based on the device identifier, the user identifier, and the cluster.

As described above, Ramasubramani describes a system in which users use a personal computer (PC) to access subscriber account information that can be later used from a mobile device to access web sites. In contrast, Applicants claim setting access privileges to the resource for a cluster of users wherein the cluster represents the user's role in an organization. An ability to assign access privileges at a cluster or group level allows different access privileges to be associated with different users of the system without the need to assign such privileges to each user individually. Thus, the system-wide access (via the mobile device) and the subscriber-based account access (via a computer) described in Ramasubramani is not germane to the amended claims.

Furthermore, Applicant's amended claims recite a request that includes two distinct elements: a "device identifier" and a "user identifier." As described above, Ramasubramani relies on a mapping of a device ID to a user's account and locates user-specific certificates using just the device ID. Only when a user accesses his personal account information from a separate device such as a personal computer to administer the personal account (e.g., change a password or provision a new certificate) does the Ramasubramani system require the presentation of a user

ID. But in that case the user is not at the mobile device, and so does not use the device ID to make such a request.

The Examiner states that Ramasubramani includes the device ID in the request “and is used to match with ID stored in 320 not 318” and that “the device ID is further associated with a subscriber ID.” Final Office Action, pg. 2. Applicants respectfully submit, however, that item 320 does not represent the user identification information as suggested in the Office Action, but instead is a reference to the certificates assigned to the user’s account for use with a particular web site. As described in Ramasubramani, when a user of a mobile device requests a certificate from the proxy server, “the device ID 86123456-10900 is extracted from the request and verified that there is an account indexed by the same device ID 86123456-10900.” Col. 9 lines 14 – 17. The device ID, in other words, is the only mechanism by which the proxy server locates a subscriber’s account. A user ID is stored on the proxy server but it is not used in the request for access.

Indeed, Ramasubramani actually teaches away from including user-specific data in a request from a mobile device: “It should be noted that the response does not request from the user a pair of username and password to permit access to the account, in fact the permission to access the account has been granted by matching the device ID in the request from the mobile device and the stored device ID of the account in the self-provision.” Col. 8 lines 43 – 50. In accordance with Ramasubramani, therefore, a user provides a user ID via a PC – not a mobile device – in order to update their account information. Col. 9, lines 28-36.

As such, Applicant respectfully submits that independent claims 1, 2 and 3, as well as those claims that depend therefrom, are patentable over the cited reference.

#### Claims 4 – 18

Independent claims 4, 11 and 18 as amended each recite, in part, locating in response to a request to access a resource context information associated with the device identifier where the context information has been assigned to the device during a previous session between the device and the resource and including access privileges associated with a cluster of uses and wherein the cluster represents the users’ role in an organization and the access privileges represent data access rights of members of the cluster to the resource.

As described above with respect to claims 1 – 3, Ramasubramani describes using a PC to access subscriber account information and request user-specific digital security certificates that can be later used to access web sites for a particular mobile device. In contrast, Applicants claim “set[ting] access privileges to the resource for a cluster of users” “wherein the cluster represents the user’s role in an organization.” The ability to assign access privileges at a group level eliminates the need to assign user-specific certificates to each user, and thus the claims are patentably distinct from the subscriber-based access rights described in Ramasubramani.

Furthermore, by maintaining context information for individual connections and making that context information available to devices in subsequent sessions, a user can move a mobile device among numerous access points without requiring re-registration to the network, while still making use of any group-level access privileges he may have acquired during a previous session. As described above with respect to claims 1 – 3, Ramasubramani maintains user and site-specific digital certificates, not context information.

As such, Applicant respectfully submits that independent claims 4, 11 and 18, as well as those claims that depend therefrom, are patentable over the cited reference.

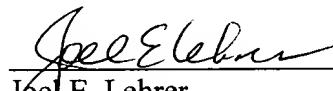
**CONCLUSION**

Applicant respectfully requests that the Examiner reconsider the application and claims in light of this Response, and respectfully submit that the claims are in condition for allowance. If the Examiner believes, in his review of this Response or after further examination, a telephonic interview would expedite the favorable prosecution of the present application, the Applicant's attorney would welcome the opportunity to discuss any outstanding issues, and to work with the Examiner toward placing the application in condition for allowance.

Respectfully submitted,

Date: March 7, 2006  
Reg. No. 56,401

Tel. No.: (617) 570-1057  
Fax No.: (617) 523-1231

  
\_\_\_\_\_  
Joel E. Lehrer  
Attorney for Applicants  
Goodwin Procter LLP  
Exchange Place  
Boston, Massachusetts 02109  
Customer No. 051414